

V. Obtaining Customer Approval for Use of CPNI

A. Soliciting Customer Approval

The Company may obtain approval through written, oral or electronic methods.

1. If the Company relies on oral approval, it bears the burden of demonstrating that such approval has been given in compliance with the FCC's regulations.
2. A customer's approval or disapproval to use, disclose, or permit access to CPNI must remain in effect until the customer revokes or limits such approval or disapproval.
3. The Company must maintain records of approval, whether oral, written or electronic, for at least one year.

B. Use of Opt-Out and Opt-In Approval Processes

1. The Company may utilize the opt-out or opt-in method to obtain approval to use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer.
2. The Company may also utilize the opt-out or opt-in method to obtain approval to disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents, to its affiliates that provide communications-related services, and to its joint venture partners and independent contractors.
3. If the Company discloses or provides access to CPNI to a joint venture partner or independent contractor, in addition to obtaining customer approval, it must enter into confidentiality agreements with such contractors or partners. The confidentiality agreement must:
 - i. Require that the independent contractor or joint venture partner use the CPNI only for the purpose of marketing or providing the communications-related services for which the Company has provided the CPNI;

- ii. Disallow the independent contractor or joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; and
- iii. Require that the independent contractor or joint venture partner have appropriate protections in place to ensure the ongoing confidentiality of consumers' CPNI.

VI. Notices Required for Use of CPNI

A. Mandatory Notices Regarding Solicitation

1. Prior to soliciting any customer approval to use, disclose, or permit access to customers' CPNI, the Company must notify the customer of the customer's right to restrict use of, disclosure of, and access to, the customer's CPNI.
2. The Company must maintain records of the notification, whether oral, written or electronic, for at least one year.
3. Content of Notice: Customer notification must provide sufficient information to enable the customer to make an informed decision whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI. The notification must:
 - i. State that the customer has a right, and the Company has a duty, under federal law, to protect the confidentiality of CPNI.
 - ii. Specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of the right to disapprove those uses, and deny or withdraw access to CPNI at any time.
 - iii. Advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, the Company may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.
 - iv. Be comprehensible and not misleading
 - v. State that any approval or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

4. If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.
5. If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.
6. The Company may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. The Company also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.
7. A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.
8. The Company's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

B. Opt-Out Notice Requirements

The Company must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except for one-time use of CPNI, as discussed in VI.E., below). The contents of any such notification must comply with the requirements of VI.A.3., above.

1. The Company must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. The Company may, in its discretion, provide for a longer period. The Company must notify customers as to the applicable waiting period for a response before approval is assumed.
 - i. In the case of an electronic form of notification, the waiting period begins to run from the date on which the notification was sent.
 - ii. In the case of notification by mail, the waiting period begins to run on the third day following the date that the notification was mailed.

2. If the Company uses the opt-out mechanism it must provide notices to its customers every two years.
3. Use of E-mail: If the Company uses e-mail to provide opt-out notices, it must comply with the following additional requirements:
 - i. The Company must have express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;
 - ii. Customers must be able to reply directly to e-mails containing CPNI notices in order to opt-out.
 - iii. Opt-out e-mail notices that are returned to the Company as undeliverable must be sent to the customer in another form before the Company may consider the customer to have received notice; and
 - iv. The subject line of the e-mail must clearly and accurately identify the subject matter of the e-mail.
 - v. The Company must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. The Company may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

D. Opt-In Notice Requirements

The Company may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements described in § VI.A.3., above.

E. Notice Requirements Specific to One-Time Use of CPNI

1. The Company may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

2. The contents of any such notification must comply with the requirements of VI.A.3., except that the Company may omit any of the following if not relevant to the limited use for which the carrier seeks CPNI:
 - i. The Company need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election.
 - ii. The Company need not advise customers that it may share CPNI with its affiliate(s) or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party.
 - iii. Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use.
 - iv. Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.
- F. Except for use and disclosure of CPNI that is permitted without customer approval as discussed above, and except for the purpose of marketing communications-related services to a customer, the Company may only use, disclose, or permit access to a customer's individually identifiable CPNI subject to opt-in approval.

VII. Company Safeguards and Recordkeeping Requirements.

A. Management Safeguards

1. Training of Company personnel will include review of this Manual by all new employees and all existing employees who have not previously done so.
2. The Company will provide additional training on an as-needed basis.
3. Company personnel will make no decisions regarding CPNI without first consulting one of the following individuals:

The CEO, COO, or CFO

The Company's personnel must obtain supervisory approval from a person listed above regarding any proposed use of CPNI.

4. In deciding whether the contemplated use of the CPNI is proper, the individual(s) listed in the previous paragraph will consult this manual, applicable FCC regulations or Compliance Guide, and, if necessary, legal counsel.
5. The person(s) listed in VII.A.3. above will personally oversee the use of approval methods and notice requirements for compliance with all legal requirements.
6. The person(s) listed in VII.A.3. above will also ensure that the Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI.
7. Any improper use of CPNI will result in disciplinary action in accordance with established Company disciplinary policies. Any improper use shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. Any company personnel making improper use of CPNI will undergo additional training to ensure future compliance.
8. The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

- i. The notice will be in the form of a letter, and will include the Company's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.
 - ii. The Company must submit the notice even if the Company offers other methods by which consumers may opt-out.
- 9. On an annual basis, a corporate officer of the Company will sign a compliance certificate (Appendix 1) stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's rules.
- 10. The Company will review these procedures on a continuing basis to ensure compliance with all FCC regulations, and will revise these procedures as needed to reflect any subsequent revisions to the applicable Rules and Regulations addressing CPNI.

B. Recordkeeping

- 1. The Company will maintain records of its own sales and marketing campaigns that use CPNI in files clearly identified as such. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.
- 2. The Company will maintain records of its affiliates' sales and marketing campaigns that use CPNI in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.

3. The Company will maintain records of all instances where it disclose or provides CPNI to third parties, or where third parties are allowed access to CPNI, in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.
4. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.
5. The Company will maintain separate files in which it will retain any court orders respecting CPNI.

C. Authentication and Procedural Safeguards

1. **Online Access to CPNI.** The Company must authenticate Customer without the use of Readily Available Biographical Information or Account Information, prior to allowing the Customer online access to CPNI related to a Telecommunications Service account. Once authenticated, the Customer may only obtain online access to CPNI related to a Telecommunications Service account through a password, as described in Section 10.C.3., that is only prompted by the Company asking for Readily Available Biographical Information, or Account Information.

The Company may choose to block access to a Customer's account after repeated unsuccessful attempts to log into that account.

2. **In-Office Access to CPNI.** The Company may disclose CPNI (including Call Detail Information) to a Customer who, in the Company's office, first presents a Valid Photo ID matching the Customer's Account Information.

APPENDIX 1

CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

_____ signs this Certificate of Compliance in accordance with § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and 47 CFR 64.2009, on behalf of _____ Telephone Company (Company). This Certificate of Compliance addresses the requirement of 47 CFR 64.2009 that the Company provide both a Certificate of Compliance and a "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR 64.2001-.2009.

On behalf of the Company, I certify as follows:

1. I am the _____ of the Company. My business address is _____.
2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to customer proprietary network information (CPNI).
3. The Company has established a system by which the status of a customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.
4. The Company trains its personnel regarding when they are authorized to use CPNI, as well as when they are not authorized to use CPNI. However, Company personnel make no decisions regarding CPNI without first consulting with management. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.
5. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.
6. The Company has a supervisory review process regarding compliance with the FCC's rules relating to protection of CPNI for outbound marketing situations. The purpose of this supervisory review process is to ensure compliance with all rules prior to using CPNI for a purpose for which customer approval is required. Company personnel, prior to making any use of

CPNI, must first consult with management regarding the lawfulness of using the CPNI in the manner contemplated. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, the FCC's Compliance Guide, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

8. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith.

9. The Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI.

10. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

Date: _____

APPENDIX 2

Employee Verification

Employee Name:

Date:

I have reviewed the Company's Customer Proprietary Network Information Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

Employee Signature

APPENDIX 3

SAMPLE OPT-OUT NOTICE

_____ Company (Company) utilizes Customer Proprietary Network Information (CPNI) when providing telecommunications products and services to its customers. CPNI is defined as information relating to the quality, technical configuration, destination and amount of use of telecommunications services, including information that may appear on a customer's bill. Information published in the telephone directory is not CPNI.

Under Federal law, telephone companies have a duty to protect this information. As a customer, you have the right at any time to restrict the use of CPNI for marketing purposes. This is considered an "Opt-Out" approach. Your approval to use CPNI may enhance the Company's ability to offer products and services tailored to your needs.

The Company proposes to use your CPNI to [Specify: (1) the information that will be used, (2) the specific entities that will receive the CPNI, (3) the purposes for which CPNI will be used].

If you wish to opt-out, you should take the following steps: [list]

Your decision to opt-out will not affect the provision of any services to which you subscribe. The Company does not and will not sell or offer such information to any third party, except as permitted under Federal Communications Commission regulations. Once you opt-out, you will remain on this list until your request otherwise.

If the Company does not receive an opt-out from you prior to the expiration of the 30-day period following the Company's sending of this notice to you, it will assume that you approve of its proposed use of your CPNI.

Red Flags and Address Discrepancies

**Compliance Manual and
Operating Procedures**

For

**Great Lakes Comnet, Inc and its subsidiary
Comlink, LLC**

**First revised copy issued October 2009
Replaces the October 2008 version
Approved by the Board of Directors on October 15, 2009**

TABLE OF CONTENTS

<u>Section No.</u>	<u>Section Title</u>	<u>Page</u>
	DEFINITIONS	1
	STATEMENT OF CORPORATE POLICY	4
	WHAT IS A RED FLAG?	5
	IDENTIFICATION OF COVERED ACCOUNTS	6
	OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM.....	7
	IDENTIFYING RED FLAGS	
	OPENING OF NEW ACCOUNTS	8
	PROTECTION OF EXISTING ACCOUNTS	16
7.	PREVENTING AND MITIGATING IDENTITY THEFT	17
8.	UPDATING THE IDENTITY THEFT PREVENTION PROGRAM.....	18
9.	ANNUAL REPORT	19
10.	SERVICE PROVIDERS	20
11.	USE OF CONSUMER REPORTS.....	21
12.	DISCIPLINARY ACTION	23
	 APPENDIX 1 – ANNUAL REPORT FORM	
	APPENDIX 2 – Employee Verification of Red Flag Compliance Manual Review	
	APPENDIX 3 – Sample Form for Credit Report Authorization	

SECTION 1

DEFINITIONS

Account: A continuing relationship established by a person with a Creditor (like the Company) to obtain a product or service for personal, family, household or business purposes, and includes the provision of services on a deferred payment basis.

Annual Report: See Section 9.

Board of Directors: The Company's board of directors, or if the Company does not have a board of directors, a designated employee at the level of senior management.

Covered Account: An Account that the Company offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. The term also includes any other Account for which there is a reasonably foreseeable risk to Customers or to the Company of Identity Theft, including financial, operational, compliance, reputation, or litigation risks (See Section 4).

SECTION 1

DEFINITIONS (CONT'D)

Consumer Report: A written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, or any other purpose authorized under 47 USC 1681 *et seq.*

Credit: The right granted by a Creditor, like the Company, to defer payment of debt or to incur debts and defer its payment or to purchase property or services on a deferred payment basis.

Creditor: A person, like the Company, who regularly extends, renews, or continues Credit, or who regularly arranges for the extension, renewal, or continuation of Credit, or any assignee of an original Creditor who participates in the decision to extend, renew, or continue Credit.

Customer: A person that has a Covered Account with a Creditor or a financial institution.

Identity Theft: A fraud committed or attempted using the Identifying Information of another person without authority.

SECTION 1

DEFINITIONS (CONT'D)

Identifying Information: A name or number that may be used, alone or in conjunction with any other information, to identify a specific person. The following are examples of Identifying Information:

- Name, Birth Date, Social Security Number, Drivers License or Identification, Alien Registration, Passport Number, Employer or Tax Identification Number;
- Unique Biometric Data, such as a Fingerprint, Voiceprint, Retina or Iris Image, or other Physical Representation;
- Unique Electronic Identification, Address, Routing Code.

Notice of Address Discrepancy: A notice from a consumer reporting agency informing the Company of a substantial difference between the address that the consumer provided and the address in the agency's file for the consumer.

Red Flag: See Section 3.

Readily Available Biographical Information: Information drawn from the Customer's life history and includes such things as the Customer's social security number (or the last four digits), mother's maiden name, home address, or date of birth.

Service Provider: A provider of a service directly to a financial institution or Creditor.

SECTION 2

STATEMENT OF CORPORATE POLICY

The policy of Great Lakes Comnet, Inc. and its subsidiary company Comlink, LLC is to comply with the letter and spirit of all laws of the United States, including those pertaining to Identity Theft contained in the Fair Credit Reporting Act, as amended, 15 USC 1681 *et seq.*, and the Federal Trade Commission's (FTC's) regulations, 16 CFR Part 681. The Company's policy is to protect against the risk of Identity Theft.

The FTC's regulations require the Company to establish a written Identity Theft Prevention Program, and to train its personnel accordingly. This Manual, in conjunction with the Company's Customer Proprietary Network Information (CPNI) Manual, constitutes the Company's written Identity Theft Prevention Program.

All personnel are required to follow the policies and procedures specified in this Manual.

- ◆ Any questions regarding compliance with applicable law and this Manual should be referred to Richard Schmoyer, 517-664-1600.
- ◆ The following individuals are responsible for oversight of the Company's Identity Theft Prevention Program:
Paul Bowman, CEO
Richard Schmoyer, CFO
John Summersett, COO
- ◆ The Company's Board of Directors Approved this first revised Manual on October 15, 2009 and replaces the original manual issued in October 2008.

SECTION 3

WHAT IS A RED FLAG?

A Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Examples of Red Flags:

- Alerts, notifications, or warnings from consumer reporting agencies, law enforcement, Customers, or victims of Identity Theft.
- Presentation of suspicious documents.
- Unusual use or suspicious activity related to a Covered Account.
- Presentation of suspicious personal identification information.

The purpose of this Manual is to set forth the Company's policies and procedures regarding Red Flags and the prevention and mitigation of Identity Theft.

SECTION 4

IDENTIFICATION OF COVERED ACCOUNTS

The Red Flag rules require the Company to periodically determine whether it offers or maintains Covered Accounts.

The Company will treat all Accounts involving the provision of service on a deferred-payment basis to the public (including residential and business services), as Covered Accounts.

The Company will, on an ongoing basis, determine whether any Accounts that it has not previously treated as Covered Accounts, should be treated as Covered Accounts, taking into consideration:

- The methods of opening Accounts;
- The methods of access to Accounts; and
- Previous experiences with Identity Theft.

SECTION 5

OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM

The Company endeavors to detect, prevent and mitigate Identity Theft (1) in connection with the opening of a Covered Account, and (2) with respect to existing Covered Accounts.

The Company will—

1. Identify relevant Red Flags for the Covered Accounts that the Company offers or maintains (see Section 6);
2. Detect Red Flags (see Section 6);
3. Take appropriate action to prevent and mitigate any detected Red Flags (see Section 7); and
4. Periodically update this Manual to reflect changes in risks to Customers and to the safety and soundness of the Company from Identity Theft (see Section 8).

SECTION 6

IDENTIFYING RED FLAGS

OPENING OF NEW ACCOUNTS

The Company has determined that a reasonably foreseeable risk of Identity Theft exists when prospective Customers seek to open new Accounts. The Company will therefore use reasonable measures to identify a person or entity that seeks to open a Covered Account.

This Section 6 therefore identifies Red Flags applicable to the opening of new Covered Accounts, and establishes the Company's method of detecting such Red Flags.

The Company will not open a Covered Account or provide any service until it is able to satisfactorily identify the prospective Customer in accordance with this Section 6. If the Company detects a Red Flag during the process of opening a Covered Account, it will place the opening of the Covered Account on hold until it can satisfactorily resolve the Red Flag.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Covered Accounts for Personal, Family or Household Purposes.

1. **Required Information:** When a prospective Customer seeks to open a Covered Account for residential service (i.e., for personal, family or household purposes), the Company will ask for the following from the prospective Customer:

- name;
- address;
- birth date;
- an unexpired government-issued identification bearing a photograph, such as a driver's license or passport.

The Company will also encourage (but not require) Customers to establish passwords as a means of protecting against potential future Identity Theft.

The Company will encourage Customers who establish passwords not to use Readily Identifiable Biographical Information.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

- A. Opening of Accounts for Personal, Family or Household Purposes (Cont'd).
 - 2. Identification Confirmation.
 - a. The Company will make a photocopy of the prospective Customer's identification, and will inspect the identification for any signs of falsification, such as:
 - misspellings;
 - a photo that does not resemble the prospective Customer;
 - inconsistencies in color, texture or images (such as erasures or smudges);
 - raised edges around a photograph indicating the placement of a second photograph over an original photograph;
 - card wear inconsistent with date of issuance (such as an identification that appears new but bears an issuance date of many years);

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Accounts for Personal, Family or Household Purposes (Cont'd).

2. Identification Confirmation (Cont'd).

b. Address Discrepancies.

If a prospective Customer provides an address to the Company that does not match the prospective Customer's identification, the Company will verify the validity of the prospective Customer's address. The following are examples of methods that the Company may utilize:

- If the prospective Customer recently moved to the area, the Company will request proof of the recent move.
- The Company may choose to order a Consumer Report with respect to the prospective Consumer as a tool to confirm identity. Before ordering a Consumer Report, the Company will obtain the prospective Customer's written approval (see Appendix 3). The Company may quiz the prospective Customer regarding non-public information contained therein. The Company may also choose to employ the services of a third-party Identity Theft detection agent.

- c.** The Company will create a record of the means used to verify a Customer's identity. The Company will retain such record until 5 years after the Account is closed. Upon disposal, the Company will completely destroy the record.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

B. Opening of Business Accounts.

For a prospective business Customer, the Company will require documents to verify the existence of the business. Such documents may include:

- Articles of Incorporation or Articles of Limited Liability Company and evidence of filing of same with the Michigan Department of Labor and Economic Growth.
- Partnership agreement.
- Trust instrument.

A sole proprietorship may use an "assumed name" document filed with the Department of Labor and Economic Growth, or the personal information of the sole proprietor.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

C. Examples of Red Flags in the Opening of New Accounts.

- 1. Suspicious Documents and Personal Identifying Information.**
 - a. Information on the identification is inconsistent with information provided by the person opening a new Covered Account.
 - b. Information on the identification is inconsistent with readily accessible information, such as a signature on a check.
 - c. Documentation that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
 - d. An address not matching any address in a Consumer Report;
 - e. Documents provided for identification appear to have been altered or forged (discussed above).

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

- C. Examples of Red Flags in the Opening of New Accounts (Cont'd).
 - 2. Unusual Use of, or Suspicious Activity Related to, the Covered Account.
 - a. A Covered Account is used in a manner inconsistent with established patterns of activity.
 - b. Usage of a Covered Account that has been inactive for a reasonably lengthy period of time.
 - c. A Customer advises that the Customer is not receiving monthly bills from the Company.
 - d. A Customer advises of unauthorized charges or transactions in connection with a Covered Account.
 - 3. The Company receives notice from a Customer, a victim of Identity Theft, law enforcement, or any other person that it may have opened an Account for a person engaged in Identity Theft.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

C. Examples of Red Flags in the Opening of New Accounts (Cont'd).

- 4. If the Company uses a Consumer Report—**
 - a. The report contains a fraud or active duty alert.**
 - b. A consumer reporting agency provides a notice of credit freeze in response to a request for a Consumer Report.**
 - c. A consumer reporting agency provides a Notice of Address Discrepancy.**
 - d. A Consumer Report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a prospective Customer.**
 - e. A recent and significant increase in the volume of inquiries.**
 - f. An unusual number of recently established Credit relationships.**
 - g. A material change in the use of Credit, especially with respect to recently established Credit relationships.**
 - h. The social security number is associated with a deceased person.**

If a Consumer Report specifies a telephone number to be used for identity verification purposes, the Company will contact the consumer using the specified telephone number.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

PROTECTION OF EXISTING ACCOUNTS

The Company has policies and procedures in place to safeguard customer proprietary network information (CPNI). The Company will continue to utilize its CPNI policies procedures as a safeguard against unauthorized access to Customer CPNI, including pre-texting. Pre-texting is the practice of obtaining call record detail and other CPNI under false pretenses. The Company also monitors suspicious transactions, and verifies change of address requests in accordance with its CPNI Compliance Manual.

The Company updates its Manual to account for changes in law, and it contains all essential information and forms to ensure the Company's compliance with CPNI regulations.

The Company will continue to follow its CPNI Compliance Manual as a means of preventing Identity Theft. The Company will also continue to improve its Identity Theft Prevention Program based on its experience with past incidents of Identity Theft, and new methods of committing Identity Theft of which it becomes aware.

The Company treats the following as Red Flags—

- Alerts, notifications, or other warnings from consumer reporting agencies or Service Providers;
- Suspicious address changes;
- The unusual use of, or other suspicious activity related to, a covered Account; and
- Notice from Customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with a Covered Account.

SECTION 7

PREVENTING AND MITIGATING IDENTITY THEFT

The Company will respond appropriately when it detects a Red Flag. In determining how to respond, the Company will consider aggravating factors that may heighten the risk of Identity Theft.

Appropriate responses include one or more of the following depending on the circumstances:

- Monitoring a Covered Account;
- Contacting the Customer;
- Changing passwords or security codes that permit access to a Covered Account;
- Reopening a Covered Account with a new account number;
- Declining to open a Covered Account for a prospective Customer;
- Closing an existing Covered Account
- Not collecting on a Covered Account; or
- Notifying law enforcement (see Section 10 of CPNI Compliance Manual).

SECTION 8

UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

The Company will update this Program periodically to reflect changes in risks to Customers or to the safety and soundness of the Company from Identity Theft.

In updating this Program, the Company will consider the following:

- The Company's experiences with Identity Theft.
- Changes in methods with which Identity Theft is committed.
- Changes in methods to detect, prevent, and mitigate Identity Theft.
- Changes in the types of Accounts that the Company offers or maintains.
- Changes in the Company's business arrangements, such as mergers, acquisitions, alliances, joint ventures, and Service Provider arrangements.

SECTION 9

ANNUAL REPORT

The Company will designate a person to be responsible for preparing an Annual Report to the Board of Directors, appropriate committee of the Board, or a designated senior-level manager.

The Annual Report will address at least the following:

- The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts.
- The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft with respect to existing Covered Accounts.
- Arrangements with Service Providers.
- Significant incidents involving Identity Theft and management's response.
- Recommendations for material changes to the Company's Identity Theft Prevention Program.

The Annual Report will be in a format similar to that contained in Appendix 1.

SECTION 10

SERVICE PROVIDERS

To the extent that the Company engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the Company will ensure that the Service Provider has its own Identity Theft Prevention Program to detect and address Red Flags.

The Company is ultimately responsible for complying with Red Flag rules even if it outsources Account-related activity to a Service Provider.

SECTION 11

USE OF CONSUMER REPORTS

To the extent that the Company uses Consumer Reports in the opening of a new Covered Account, it will comply with this Section 11.

If the Company receives a Notice of Address Discrepancy from a consumer reporting agency, the Company must form a reasonable belief that the Consumer Report relates to the prospective Customer about whom it has requested the report.

The Company will do one or more of the following to determine whether it has a reasonable belief that the Consumer Report relates to the prospective Customer about whom it has requested the report:

- Compare the information in the Consumer Report with information the Company uses to verify the prospective Customer's identity.
- Compare the information in the Consumer Report provided by the consumer reporting agency with information the Company obtains from third-party sources.
- Verify with the prospective Customer.

SECTION 11

USE OF CONSUMER REPORTS (CONT'D)

If the Company has reasonably confirmed that an address relates to the prospective Customer about whom it has requested the report, it must furnish the address for the prospective Customer to the consumer reporting agency from whom it received the Notice of Address Discrepancy.

SECTION 12

DISCIPLINARY ACTION

Any failure to follow this Manual will result in appropriate disciplinary action in accordance with established Company disciplinary policies. Such failures shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. The Company will also require additional training to ensure future compliance.

APPENDIX 1

ANNUAL REPORT FORM

**To be completed by the Board of Directors,
appropriate committee of the Board of
Directors, or a designated senior-level
manager.**

ANNUAL REPORT FOR _____

This Annual Report constitutes _____ Company's (Company) obligation under the Federal Trade Commission's (FTC) regulations and guidelines, 16 CFR Part 681, to produce an Annual Report to address the Company's compliance with the FTC's Red Flag regulations.

1. Effectiveness of Policies and Procedures

a. Opening of Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts:

b. Existing Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with existing Covered Accounts:

2. Arrangements with Service Providers

The Company [does/does not] outsource some services to third party Service Providers related to Covered Accounts. [If the Company "does," list them and state:] The Company has taken the following measures to ensure that its Service Provider(s) have Identity Theft Prevention Program(s) to detect and address Red Flags:

3. Significant Incidents Involving Identity Theft

The Company reports the following significant incidents involving Identity Theft and management's response:

4. Recommendations for Material Changes to the Program

The Company should consider the following changes to its Identity Theft Prevention Program.

[Typed Name]

[Typed Title]

Dated: _____

APPENDIX 2

EMPLOYEE VERIFICATION OF RED FLAG COMPLIANCE MANUAL REVIEW

Employee Verification

Employee Name:

I have reviewed the Company's Red Flag and Address Discrepancies Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

Employee Signature

Date

APPENDIX 3

SAMPLE FORM FOR CREDIT REPORT AUTHORIZATION

CREDIT REPORT AUTHORIZATION AND RELEASE

Authorization is hereby granted to _____ (Company)
to obtain a standard factual data credit report through a consumer credit
reporting agency chosen by Company.

Social Security Number

Date of Birth

Last Name

First Name

M.I.

Street

City

State

Zip Code

Phone Number

Signature

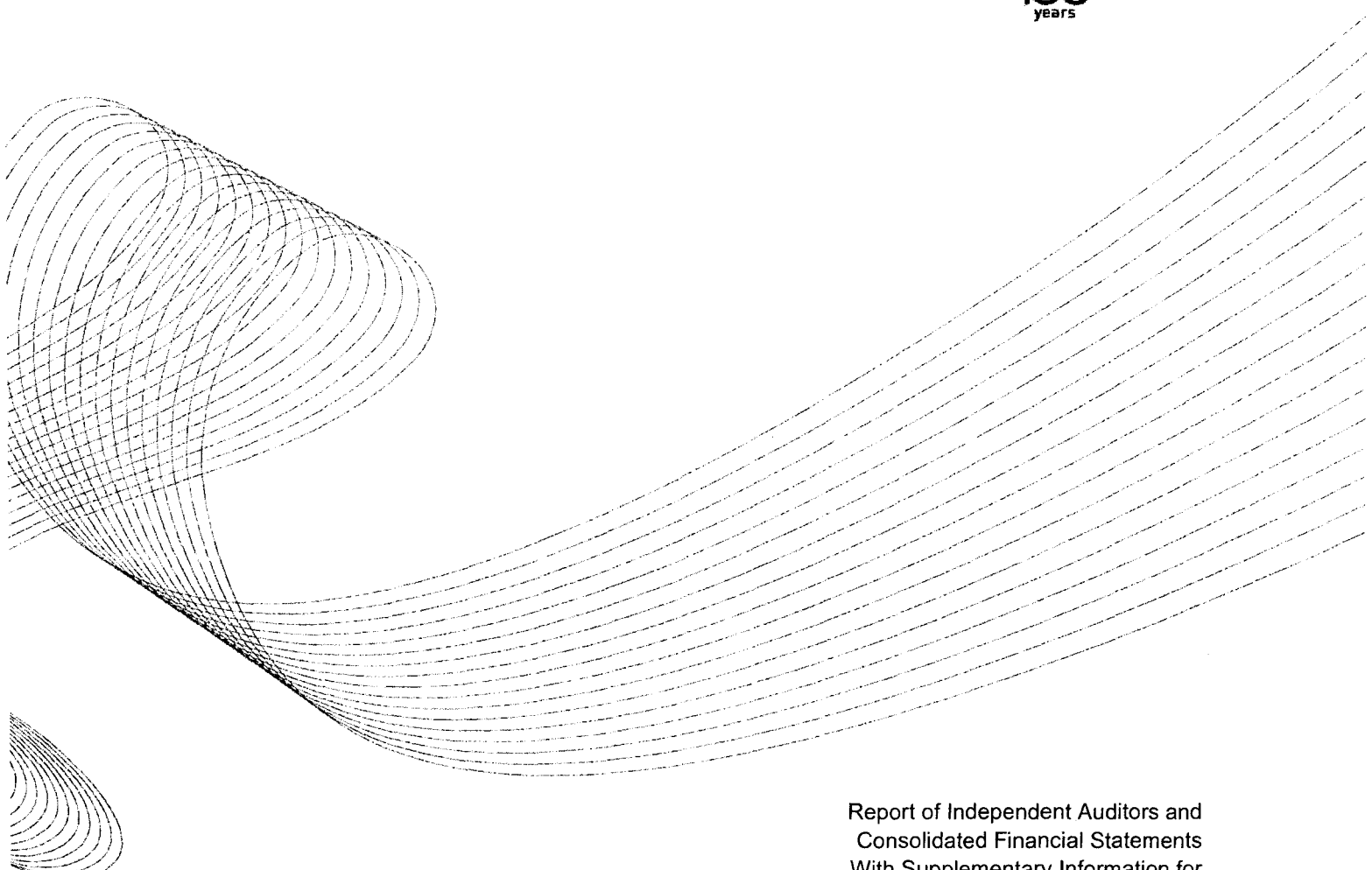
Date

(610) Functionality in Emergency Situations

Carrier is able to remain functional in an emergency situation through the use of back-up power to ensure functionality without an external power source. Carrier has backup battery reserve in its central office, which enables it to provide service for a minimum of eight (8) hours. Carrier's service is consistent with the prior obligations to provide service in emergency situations as set forth in §54.202(a)(2) and Rule 46 of the Michigan Public Service Commission's Service Quality Rules (2000 AC, R 484.546), and its network is engineered to provide maximum capacity in order to handle excess traffic in the event of traffic spikes resulting from emergency situations. Carrier has redundancy in its network for use for use in re-routing traffic when facilities are damaged.

Westphalia Telephone Company was not provided a management letter for either their 2012 or 2011 audited financial statements. Located on pages 27 of this PDF file is the page from the exit memo from our external auditors for the 2012 audited financial statements that is the communication with those charges with governance. As you can see, it is addressed to Great Lakes Comnet. Westphalia Telephone Company is a subsidiary of Clinton County Telephone Company and Clinton County Telephone Company is a subsidiary of Great Lakes Comnet. As such, Westphalia Telephone Company is covered by the Great Lakes Comnet exit memo. An exit memo was not provided by our auditors for the 2011 audited financial statements.

Sincerely,
David Meyer
Senior Accountant
Westphalia Telephone Company
(517) 664-1900
dmeyer@comlink.net

A large, abstract graphic composed of numerous thin, curved lines that sweep across the upper half of the page. The lines originate from the left side and curve towards the right, creating a sense of motion and depth. Some lines are more densely packed, forming a bulbous shape on the left, while others are more spread out, trailing off towards the right.

Report of Independent Auditors and
Consolidated Financial Statements
With Supplementary Information for

**Clinton County Telephone
Company and Subsidiaries**

December 31, 2012 and 2011

MOSS ADAMS_{LLP}

Certified Public Accountants | Business Consultants

Acumen. Agility. Answers.

CONTENTS

	PAGE
REPORT OF INDEPENDENT AUDITORS	1-2
CONSOLIDATED FINANCIAL STATEMENTS	
Consolidated balance sheets	3-4
Consolidated statements of income	5
Consolidated statements of changes in stockholder's equity	6
Consolidated statements of cash flows	7-8
Notes to consolidated financial statements	9-18
SUPPLEMENTARY INFORMATION	
Report of independent auditors on supplementary information	19
Consolidating balance sheet	20-21
Consolidating statement of income	22

REPORT OF INDEPENDENT AUDITORS

Board of Directors
Clinton County Telephone Company

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of Clinton County Telephone Company and its subsidiaries, which comprise the consolidated balance sheet as of December 31, 2012, and the related consolidated statements of income, changes in stockholder's equity, and cash flows for the year then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these consolidated financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate for the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

REPORT OF INDEPENDENT AUDITORS
(continued)

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of Clinton County Telephone Company and its subsidiaries as of December 31, 2012, and the results of their operations and their cash flows for the year then ended in accordance with accounting principles generally accepted in the United States of America.

Other Matter

The consolidated financial statements of Clinton County Telephone Company for the year ended December 31, 2011, were audited by another auditor whose report dated April 24, 2012, expressed an unmodified opinion on those statements.

MOSS ADAMS LLP

Spokane, Washington
March 26, 2013